C

Computer Network Attack: Types, Warning Signs, and Incident Response

A computer network attack attempts to gain unauthorized access or impair the confidentiality, integrity, or availability of systems, services, communications, or data.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

A **computer network attack** is malicious activity that attempts to gain unauthorized access or impair the confidentiality, integrity, or availability of systems, services, communications, or data. It can target one device, an identity platform, cloud environment, application, network segment, service provider, or the path between them.

NIST definitions include attempts to collect, disrupt, deny, degrade, destroy, or maliciously control information-system resources. An attack does not need to cause a visible outage; quiet credential theft and data access can be equally serious.

Common attack types

- **Credential attacks:** phishing, password spraying, token theft, MFA manipulation, and session replay.

- **Exploitation:** abuse of vulnerable internet services, applications, devices, or unsafe configuration.
- **Malware and remote access:** loaders, backdoors, ransomware, or legitimate administration tools used without authorization.
- **Interception and redirection:** rogue Wi-Fi, DNS or routing manipulation, proxy abuse, and man-in-the-middle attacks.
- **Denial of service:** traffic, requests, or resource exhaustion that makes a service unavailable.
- **Supply-chain compromise:** a trusted vendor, update, dependency, account, or management system becomes the entry path.

How an intrusion may progress

An attacker may discover exposed assets, obtain initial access, establish persistence, increase privilege, evade detection, steal credentials, move laterally, collect data, exfiltrate it, disrupt operations, or extort the owner. Not every attack follows every stage or a fixed order. Defenders should build a timeline from evidence instead of forcing events into a template.

Signals worth investigating

- new sign-ins, MFA methods, tokens, administrator accounts, or access from unusual devices;
- unexpected exposed services, firewall changes, DNS records, routes, proxies, or remote-management tools;
- scanning, repeated authentication failures, abnormal east-west connections, or access outside a host's role;
- security agents stopped, audit records cleared, clocks changed, or logging interrupted;
- unusual archive creation, bulk reads, outbound transfer, encryption, deletion, or service degradation.

One slow service, blocked connection, or failed login is not proof of attack. Correlate endpoint, identity, network, cloud, application, DNS, and business records.

First response steps

1. **Declare and coordinate.** Assign an incident lead, record decisions, and involve service owners, legal, privacy, communications, and providers as required.
2. **Preserve evidence.** Protect volatile data and authentication, endpoint, firewall, DNS, flow, application, cloud, and configuration logs before retention expires.
3. **Scope before broad changes.** Identify affected identities, systems, data, segments, providers, time range, and known-good administration paths.
4. **Contain safely.** Isolate confirmed hosts, revoke exposed sessions and credentials, block verified malicious infrastructure, or rate-limit an attacked service.
5. **Remove the cause.** Close the entry path, remove persistence, rebuild untrusted systems, and search for related activity elsewhere.
6. **Recover in stages.** Restore from verified sources, validate security controls, monitor closely, and keep an option to contain again.

Do not reboot, wipe, rotate every credential, or block large address ranges reflexively. Those actions can destroy evidence, interrupt safety-critical service, alert the attacker, and create avoidable outages.

Risk reduction

- maintain an external asset inventory and patch internet-facing systems quickly;
- use phishing-resistant MFA, least privilege, separate administration, and protected recovery accounts;
- segment networks and restrict management interfaces and outbound paths;
- centralize protected endpoint, identity, network, cloud, and application telemetry;
- test DDoS, backup, isolation, credential-revocation, and provider escalation procedures;

- review suppliers, remote access, secrets, dependencies, and configuration drift.

Reference: NIST CSRC: Attack.

Network attack FAQ

Is blocking one IP enough?

Rarely. Infrastructure changes, and the attacker may already have credentials or persistence. Treat the block as containment, not root-cause removal.

When should outside help be called?

Early when safety, regulated data, material outage, extortion, privileged compromise, or insufficient internal capacity is involved.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com